DETAILED ACTION

1. This action is in response to application amendments filed on 10-7-2009.

2. Claims **1, 3 - 20** are pending. Claim **2** has been cancelled. Claims **1, 7, 19** are independent. The application was filed on 2-26-2004.

Response to Arguments

3. Applicant's arguments have been fully considered but they were not persuasive.

3.1 The 112 rejection will be withdrawn due to remarks.

3.2 Applicant argues that the referenced prior art does not disclose, *software signature site*.

The specification on page 6, paragraph [0021] discloses that the software signature site is the manufacturer of the software and that the manufacturer of the software is also the manufacturer of the control unit or entity.

England prior art discloses a manufacturer of software. And, England prior art discloses that the software manufacturer signs the software (such as a boot block). Since it is the manufacturer of the software (England discloses) therefore it is the software signature site as per specification. In addition, England prior art discloses that the manufacturer has a public/private key pair. That particular private key is used to sign the software. (see England col. 7, line 63 - col. 8, line 37: manufacturer (CPU, controlling entity for control unit, OS software manufacturer) certificate generated with

public/private keys; manufacturer's public/private key pair)

The England prior art discloses a software signature site and a public/private key pair used for signing software.

3.3 Applicant argues that the referenced prior art does not disclose, *a public key of a software signature site.*

England prior art discloses a manufacturer of the software. And, England discloses that the manufacturer has a public/private key pair. The particular private key is used to sign the software. (see England col. 7, line 63 - col. 8, line 37: manufacturer (CPU, control entity, OS software manufacturer) certificate generated with public/private keys; manufacturer's public/private key pair)

3.4 Applicant argues that the referenced prior art does not disclose, *a secret key of a control entity of a trust center.*

A 103 rejection based on multiple (3) references is a legitimate technique according to the MPEP. The current application is rejected based on the England, David and the Wong prior art references. Both references are in a same field of endeavor as the claimed invention, concerning the processing of content certification. The 103 rejection allows portions of a claimed invention to come from different prior art references.

England prior art discloses a trusted third party and the third party key is used to sign software. (England col. 8, line 66 - col. 9, line 3: components signed by a trusted third party)

David prior art discloses the generation of a certificate using a public key and a secret key. (David col. 5, lines 43-54: prior generated public keys for device updated; creates a unique device certificate by digitally signing public key with manufacturer's secret key)

And, Wong prior art discloses a vehicle control unit and controlling a vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit)

Claim Rejections – 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims **1, 3 - 20** are rejected under 35 U.S.C. 103 (a) as being unpatentable over **England et al.** (US Patent No. **6,330,670**) in view of **David** (US Patent No. **6,292,892**) and further in view of **Wong et al.** (US Patent No. **5,957,985**)

Regarding Claim 1, England discloses a method comprising providing software for use by a control unit;

a) before its use, signing the software against falsification (see England col. 8, lines 34-37: boot block signed by OS manufacturer; (boot block processed before

execution or use of software); col. 11, lines 47-51: boot block and all loaded components signed by a trusted source and provided with a certificate), using a secret or private key of a software signature site (see England col. 8, line 66 - col. 9, line 2: software developer or manufacturer digitally signs software before use; private (secret) key of manufacturer's CPU (control entity)), according to a public-key method; (see England col. 7, line 63 - col. 8, line 14: key pair (public/private keys) generated and used)

Furthermore, England discloses:

b) checking the signed software for integrity, using a public key complementary to the secret key of the software signature site; (see England col. 11, lines 54-59: checks digital signature of a component before loading it; signature valid then component has not been compromised and loaded)

As per previous Remarks, the invention requires the following in subsequent claims: a signed digital certificate; identification for a digital certificate; a trust center or a trusted third party.

Furthermore, England discloses a signed digital certificate from the manufacturer of the control unit (CPU) and OS software. (see England col. 11, lines 47-51: boot block and all loaded components signed by a trusted source and provided with a certificate)

This is equivalent to disclosure in the specification on page 6, paragraph [0021], lines 3-6, that software signature certificate is generated and signed by the manufacturer of software.

Furthermore, England discloses a digital certificate containing an identification number for a control entity. (see England col. 8, lines 26-28; col. 9, lines 4-10: software identity;

identify of an authenticated OS)

This is equivalent to the specification on page 3, paragraphs [0010] and [0012], which discloses that the clearing code certificate contains an identifier and the capability to restrict usage to a particular control entity.

Furthermore, England discloses a trust center or a trusted third party for certificate signing. (see England col. 8, line 66 - col.9, line 3: trusted third party (use digital signature for authentication))

This is equivalent to the disclosure in specification on page 6, paragraph [0022], that a trust center or trusted third party generates certificates.

England does not specifically disclose generating a certificate using a public key and a secret key.

However, David discloses wherein generating a signature certificate using the public key of the signature site and a secret key of a control entity, according to a public-key method. (David col. 5, lines 43-54: device for prior generated public keys updated; creates a unique device certificate by digitally signing public key with manufacturer's secret key)

It would have been obvious to one of ordinary skill in the art to modify England for generating a certificate using a public key and a secret key as taught by David. One of ordinary skill in the art would have been motivated to employ the teachings of David to ensure secured communications between a system incorporating a secure device and a device in remote communications with the device. (see David col. 1, lines 14-20)

England-David does not specifically disclose a control unit of a vehicle. However, Wong discloses a control unit of a vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: control unit; software for vehicle control unit)

It would have been obvious to one of ordinary skill in the art to modify England-David for a control unit of a vehicle as taught by Wong. One of ordinary skill in the art would have been motivated to employ the teachings of Wong for a commonly accepted standard for a device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Regarding Claim 3, England discloses the method according to claim 1, wherein one of a control entity certificate and a trust center certificate is generated according to a public-key method by using the secret key of the control entity. (see England col. 7, line 63 - col. 8, line 14: manufacturer (CPU, control entity) certificate generated; manufacturer public/private key pair usage)

Regarding Claim 4, England discloses the method according to claim 1, wherein clearing code data are signed using a secret key of a clearing code site according to a public key method. (see England col. 8, lines 26-37; col. 9, lines 4-10: software identify (clearing code site identifier); uniquely determines OS identity signed by manufacturer; col. 8, lines 7-12: public/private key pair usage)

Regarding Claim 5, England discloses the method according to claim 1, wherein a

clearing code site signature certificate is generated using the secret key of the control entity of the trust center according to a public-key method. (see England col. 8, lines 26-37; col. 9, lines 4-10: software identify (clearing code site identifier); uniquely determines OS identity signed by manufacturer; col. 8, lines 7-12: public/private key pair usage)

Regarding Claim 6, England discloses the method according to claim 3, wherein the trust center certificate is protected against falsification and exchange, in a protected memory area in the control unit. (see England col. 8, lines 26-28; col. 9, lines 4-10: internal software identity register; col. 8, line 66 - col. 9, line 3: trusted third party to digitally sign all components)

Regarding Claim 7, England discloses a method of providing software for use by a control unit of a vehicle, said method comprising:

a) before its use by the control unit, signing the software against falsification (see England col. 8, lines 34-37: boot block signed by OS manufacturer; col. 11, lines 47-51: boot block and all loaded components signed by a trusted source and provided with a certificate; sign boot code), using a secret or private key of a software signature site (see England col. 8, line 66 - col. 9, line 2: software developer or manufacturer signs software), according to a public-key method; (see England col. 7, line 63 - col. 8, line 14: key pair (public/private keys) generated and used; public key of manufacturer for CPU (control entity))

Furthermore, England discloses the following:

b) checking the signed software for integrity, using a public key complementary to the secret key of the software signature site; (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised)

c) wherein a clearing code site signature certificate, a software signature certificate, the clearing code data and their signature as well as the software and its signature are stored in the control unit; (see England col. 7, lines 50-54: storage of keys, certificates; manufacture equips the CPU with a pair of public and private keys that is unique to CPU; certificate contains public key)

Furthermore, England discloses a trust center or a trusted third party for certificate signing. (see England col. 8, line 66 - col.9, line 3: trusted third party)
This is equivalent to the disclosure in specification on page 6, paragraph [0022], that a trust center or trusted third party generates certificates.

England does not specifically disclose software signature certificate is generated using the public key of the software signature site and a secret key of a control unit. However, David discloses wherein generating a signature certificate using the public key of the signature site and a secret key of a control entity, according to a public-key method. (David col. 5, lines 43-54: device for prior generated public keys updated; creates a unique device certificate by digitally signing public key with manufacturer's secret key)

It would have been obvious to one of ordinary skill in the art to modify England for generating a certificate using a public key of the signature site and a secret key of a control entity as taught by David. One of ordinary skill in the art would have been motivated to employ the teachings of David to ensure secured communications between a system incorporating a secure device and a device in remote communications with the device. (see David col. 1, lines 14-20)

England-David does not specifically disclose a control unit of a vehicle. However, Wong discloses a control unit of a vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit)

It would have been obvious to one of ordinary skill in the art to modify England-David for a control unit of a vehicle as taught by Wong. One of ordinary skill in the art would have been motivated to employ the teachings of Wong for a commonly accepted standard for a device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Regarding Claim 8, England discloses the method according to claim 1, wherein the software signature certificate includes at least one validity restriction. (see England col. 8, lines 26-28; col. 9, lines 4-10: internal software identity register (validity restriction); col. 8, line 66 - col. 9, line 3: trusted third party to digitally sign all components)

Regarding Claim 9, England discloses the method according to claim 5, wherein the clearing code site signature certificate includes at least one validity restriction, a

restriction to a particular control unit which is designated by means of an identification number stored in the control unit in an invariable manner, and a restriction to a identification number. (see England col. 8, lines 26-28; col. 9, lines 4-10: internal software identity register (validity restriction); uniquely determines the OS; col. 8, line 66 - col. 9, line 3: trusted third party to digitally sign all components)

England does not specifically disclose a control unit of a vehicle.

However, Wong discloses a control unit of a vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit)

It would have been obvious to one of ordinary skill in the art to modify England for a control unit of a vehicle as taught by Wong. One of ordinary skill in the art would have been motivated to employ the teachings of Wong for a commonly accepted standard for a device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Regarding Claim 10, England discloses the method according to claim 1, wherein the software signature certificate is checked for integrity according to a public-key method, using a public key of the trust center. (see England col. 8, line 66 - col. 9, lines 3: all components digitally signed by a trusted third party; col. 8, lines 7-12: public/private usage for manufacturer)

Regarding Claim 11, England discloses the method according to claim 1, wherein the signed software is checked for integrity according to a public key method, using the public key of the software signature site contained in the software signature certificate. (see England col. 11, lines 54-59: checks signature of a component before loading it; if

signature valid then component has not been compromised; col. 8, lines 7-12: public/private key pair usage; checked for validity)

Regarding Claim 12, England discloses the method according to claim 5, wherein the clearing code site signature certificate is checked for integrity according to a public key method, using a public key of the trust center. (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised; col. 8, lines 7-12: public/private key pair usage; checked for validity)

Regarding Claim 13, England discloses the method according to claim 4, wherein the signed clearing code data are checked for integrity according to a public key method, using a public key of the clearing code site contained in the clearing code site signature certificate. (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised; col. 8, lines 7-12: public/private key pair usage; checked for validity)

Regarding Claim 14, England discloses the method according to claim 1, wherein the control unit is equipped with a sequence-controlled microprocessor that implements one of the above-described methods.

England does not specifically disclose a motor vehicle control unit.

However, Wong discloses a motor vehicle control unit. (see Wong col. 2, lines 21-29: vehicle processor (microprocessor); col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col.

7, lines 35-39: software for vehicle control unit)

It would have been obvious to one of ordinary skill in the art to modify England for a motor vehicle control unit as taught by Wong. One of ordinary skill in the art would have been motivated to employ the teachings of Wong for a commonly accepted standard for a device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Regarding Claim 15, England discloses a control unit, which implements a method according to claim 1.

England does not specifically disclose a motor vehicle.

However, Wong discloses a motor vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit)

It would have been obvious to one of ordinary skill in the art to modify England for a motor vehicle as taught by Wong. One of ordinary skill in the art would have been motivated to employ the teachings of Wong for a commonly accepted standard for a device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Regarding Claim 16, England discloses a data processing system, which implements a method according to claim 1.

England does not specifically disclose a motor vehicle.

However, Wong discloses a motor vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit)

It would have been obvious to one of ordinary skill in the art to modify England for a motor vehicle as taught by Wong. One of ordinary skill in the art would have been motivated to employ the teachings of Wong for a commonly accepted standard for a device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Regarding Claim 17, England discloses a computer program product sequence control of a data processing system, which implements the method according to claim 1. England does not specifically disclose a motor vehicle.
However, Wong discloses a motor vehicle or motorcycle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit)

It would have been obvious to one of ordinary skill in the art to modify England for a motor vehicle or motorcycle as taught by Wong. One of ordinary skill in the art would have been motivated to employ the teachings of Wong for a commonly accepted standard for a device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Regarding Claim 18, England discloses a data carrier, comprising a computer program product according to claim 17. (see England col. 10, lines 55-59: software; computer program product)

Regarding Claim 19, England discloses a method of providing software for use by a control unit of a vehicle, said method comprising:

a) storing, a software signature certificate; receiving, signed software; (see England col. 7, lines 50-54: storage of keys, certificates; manufacture equips the CPU with a pair of public and private keys that is unique to CPU)

Furthermore, England discloses the following:

b) checking, whether the software signature certificate has been changed or manipulated; (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised)

c) checking, whether the signed software has been changed or manipulated. (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised)

England does not specifically disclose a control unit of a vehicle.

However, Wong discloses a control unit of a vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 32-39: control unit, vehicle)

It would have been obvious to one of ordinary skill in the art to modify England for a control unit of a vehicle as taught by Wong. One of ordinary skill in the art would have been motivated to employ the teachings of Wong for a commonly accepted standard for a device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Regarding Claim 20, England discloses the method of claim 19, further comprising:

a) storing, a trust center certificate that includes a public key and a signature generated using a secret key of a trust center; (see England col. 7, lines 50-54:

storage of keys, certificates; manufacture equips the CPU with a pair of public and private keys that is unique to CPU)

Furthermore, England discloses the following:

b) storing, a clearing code site signature certificate that includes a second public key and a second signature; (see England col. 7, lines 50-54: storage of keys, certificates; manufacture equips the CPU with a pair of public and private keys that is unique to CPU)

c) wherein the software signature certificate includes a third public key and a third signature; (see England col. 7, lines 50-54: storage of keys, certificates; manufacture equips the CPU with a pair of public and private keys that is unique to CPU)

England does not specifically disclose a control unit of a vehicle. However, Wong discloses a control unit of a vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 32-39: control unit, vehicle)

It would have been obvious to one of ordinary skill in the art to modify England for a control unit of a vehicle as taught by Wong. One of ordinary skill in the art would have been motivated to employ the teachings of Wong for a commonly accepted standard for a device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser Moazzami/
Supervisory Patent Examiner, Art Unit 2436

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
January 4, 2010